|  |  |
| --- | --- |
| Uninstall CSF Firewall | Config Server Firewall (CSF) |

# Introduction

Config Server and Security (CSF) est un pare-feu open source pour les systèmes Linux.   
Il fournit non seulement les fonctionnalités de base d'un pare-feu, mais offre également un large éventail de fonctionnalités complémentaires telles que la détection de connexion/intrusion, les vérifications d'exploits, une protection contre le ping de la mort (*ping of death*) et bien plus encore.

# Installation de CSF

La première étape est l’installation de certaines dépendances …  
**>> sudo apt update  
>> sudo apt install wget libio-socket-ssl-perl git perl iptables libnet-libidn-perl libcrypt-ssleay-perl \  
 libio-socket-inet6-perl libsocket6-perl sendmail dnsutils unzip**

Étant donné que CSF n'est pas inclus dans les référentiels Debian par défaut, on doit l'installer manuellement.   
Pour continuer, il fut télécharge le fichier tarball CSF qui contient tous les fichiers d'installation …  
**>> cd /tmp   
>> wget http://download.configserver.com/csf.tgz**

On extrait le fichier compressé …  
**>> tar -xvzf csf.tgz**

Cette commande crée le dossier csf …  
**>> cd csf**

On installe ensuite CSF en exécutant le script d'installation …  
**>> sudo bash install.sh**

CSF est installé.   
Toutefois, on doit vérifier que les tables requises sont chargées.   
Pour s’en assurer …  
**>> sudo perl /usr/local/csf/bin/csftest.pl  
Testing ip\_tables/iptable\_filter...OK  
Testing ipt\_LOG...OK  
Testing ipt\_multiport/xt\_multiport...OK  
Testing ipt\_REJECT...OK  
Testing ipt\_state/xt\_state...OK  
Testing ipt\_limit/xt\_limit...OK  
Testing ipt\_recent...OK  
Testing xt\_connlimit...OK  
Testing ipt\_owner/xt\_owner...OK  
Testing iptable\_nat/ipt\_REDIRECT...OK  
Testing iptable\_nat/ipt\_DNAT...OK  
  
RESULT: csf should function on this server**

# Configuration de CSF

Une configuration supplémentaire est nécessaire. Ensuite, on doit modifier quelques paramètres pour activer CSF.

On modifie le fichier de configuration …  
**>> sudo nano /etc/csf/csf.conf**

On modifie la valeur de la directive TESTING de 1 à 0 …  
**TEST = "0"**Cette directive désactive les tests CSF.

Ensuite, on définit la directive RESTRICT\_SYSLOG sur 3 afin de restreindre l'accès à rsyslog/syslog uniquement aux membres du groupe syslog RESTRICT\_SYSLOG\_GROUP …  
**RESTRICT\_SYSLOG = "3"**

La prochaine étape consiste à ouvrir les ports TCP et UDP.  
On doit le faire à l’aide des directives …

* TCP\_IN ;
* TCP\_OUT ;
* UDP\_IN   
  et
* UDP\_OUT.

Par défaut, les ports suivants sont ouverts.

* TCP\_IN = "20,21,22,25,53,80,110,143,443,465,58,993,995 " ;
* TCP\_OUT = " 20,21,22,25,53,80,110,113,443,587,993,995 " ;
* UDP\_IN = "20,21,53,80,443" ;
* UDP\_OUT = "20,21,53,113,123"

Une bonne pratique suggère de n’ouvrir que les ports nécessaires sur un serveur (ceux que l’on utilise seulement).   
il est donc recommandé de supprimer tous les ports inutiles et de laisser ceux qui sont utilisés par les services exécutés sur le système.

Une fois les ports spécifiés, on doit recharge CSF …  
**>> sudo csf -r**

Pour lister toutes les règles de table IP définies sur le serveur …  
**>> sudo csf -l**

Comme dernière étape, on doit démarrer et activer le pare-feu CSF au démarrage …  
**>> sudo systemctl start csf  
>> sudo systemctl enable csf**

On peut vérifier que le pare-feu est bien en cours d'exécution …  
**>> sudo systemctl status csf**

# Blocage et autorisation d’adresses IP

L'une des fonctionnalités clés d'un pare-feu est la possibilité d'autoriser ou de bloquer l'accès au serveur.   
Avec CSF, on peut créer des listes blanche (autoriser) et noire (abandonner) ou ignorer les adresses IP en modifiant des fichiers de configuration.

Les fichiers à modifier sont …

* csf.allow
* csf.deny
* csf.ignore

## Blocage d’adresses IP

Pour bloquer une adresse IP, on doit modifier le fichier de configuration csf.deny …  
**>> sudo nano /etc/csf/csf.deny**

On spécifie dans ce fichier les adresses IP que l’on souhaite bloquer.   
Il est possible de spécifier les adresses IP ligne par ligne …  
**192.168.1.50   
192.168.1.120**ou on utiliser la notation CIDR pour bloquer un sous-réseau entier …  
**192.168.1.0/24**

## Autorisation d’adresses IP

Pour autoriser une adresse IP à l’aide d’iptables et l'exclure de tous les filtres ou blocs, on doit modifier le fichier de configuration csf.allow …  
**>> sudo nano /etc/csf/csf.allow**

Il est possible, dans ce fichier, de répertorier une adresse IP par ligne ou utiliser la notation CIDR.

**Remarque** …  
Une adresse IP sera autorisée même si elle est explicitement définie dans le fichier de configuration csf.deny.   
Pour s’assurer qu'une adresse IP est bloquée par une liste noire, il est important qu'elle n'est pas répertoriée dans le fichier csf.allow.

## Exclusion d’adresses IP

De plus, CSF offre la possibilité d'exclure une adresse IP des tables IP ou des filtres.   
Toute adresse IP dans le fichier csf.ignore sera exemptée des filtres iptables.  
Elle ne pourra être bloquée que s'il est spécifié dans le fichier csf.deny.

Pour exempter une adresse IP des filtres, on doit le faire en modifiant le fichier csf.ignore.  
Encore une fois, on peut lister les adresses IP ligne par ligne ou utiliser la notation CIDR .

Référence

<https://www.tecmint.com/install-config-server-firewall-debian-ubuntu/>